

Suzuki-invariant codes from the Suzuki curve

Abdulla Eid, Hilaf Hasson, Amy Ksir, Justin Peachey*

November 27, 2014

Abstract

In this paper we consider the Suzuki curve $y^q + y = x^{q_0}(x^q + x)$ over the field with $q = 2^{2m+1}$ elements. The automorphism group of this curve is known to be the Suzuki group $Sz(q)$ with $q^2(q-1)(q^2+1)$ elements. We construct AG codes over \mathbb{F}_{q^4} from a $Sz(q)$ -invariant divisor D , giving an explicit basis for the Riemann-Roch space $L(\ell D)$ for $0 < \ell \leq q^2 - 1$. These codes then have the full Suzuki group $Sz(q)$ as their automorphism group. These families of codes have very good parameters and are explicitly constructed with information rate close to one. The dual codes of these families are of the same kind if $2g - 1 \leq \ell \leq q^2 - 1$.

1 Introduction

The Suzuki curve has been a source of very good error-correcting codes. Codes constructed from the Suzuki curve have been studied, for example, in [1], [3], [7] (one-point codes), and [9] (two-point codes) and shown to have very good parameters. Furthermore, the Suzuki curve has a very large automorphism group for its genus, namely the Suzuki group $Sz(q) = {}^2B_2$ of order $q^2(q-1)(q^2+1)$. The one-point and two-point codes previously studied had automorphism groups which were not the full Suzuki group. In this paper, we construct a family of codes on the Suzuki curve with the full Suzuki group as its group of automorphisms. We find that our codes also have very good parameters.

The outline of our paper is as follows: In Section 2 we start with some preliminaries about the Suzuki curve. In Section 3 we give an explicit basis for the Riemann-Roch space $L(\ell D)$ for $0 < \ell \leq q^2 - 1$, where the divisor D is the sum of all \mathbb{F}_q -rational points of the Suzuki curve. In Section 4 we construct families of AG-codes with good parameters, and with the full Suzuki group as automorphism group. These families are significant because they are explicitly constructed in a polynomial-time with rate close to one. In Section 5 we find the dual codes of the codes constructed in Section 4 and we find the conditions of these codes to be of the same kind, isodual, and iso-orthogonal.

The authors would like to thank Rachel Pries for organizing the workshop on rational points on Suzuki Curves in which this paper was conceived.

*This work was conducted at the Mathematics Department, Colorado State University, Summer 2011, funded by NSF grant DMS-11-01712

2 Preliminaries

Let $m \geq 1$ be an integer, $q_0 := 2^m$, $q := 2^{2m+1} = 2q_0^2$, and let X_m denote the smooth projective curve with affine plane equation

$$y^q + y = x^{q_0}(x^q + x) \quad (2.1)$$

over \mathbb{F}_q . Then, X_m has a singular projective plane model Y_m in $\mathbb{P}_{\mathbb{F}_2}^2$ with the homogeneous equation

$$y^q t^{q_0} + y t^{q+q_0-1} = x^{q+q_0} + x^{q_0+1} t^{q-1}$$

in homogeneous coordinates $[t : x : y]$. This curve has been studied, for example, in [2] and [8] and it has been shown in [5] that the curve has a smooth projective embedding in \mathbb{P}^4 . Moreover, X_m has a very large automorphism group for its genus, namely the Suzuki group $\text{Sz}(q)$ of order $q^2(q-1)(q^2+1)$. As such, X_m is known as the Suzuki curve. We summarize these properties as well as several others shown in [4] and [7] in the following proposition:

Proposition 2.1. *Let $m \geq 1$ be an integer, $q_0 := 2^m$, $q := 2^{2m+1} = 2q_0^2$, and let X_m denote the Suzuki curve. Then,*

1. *The smooth projective curve X_m has a single point P_∞ above the singularity at infinity $[0 : 0 : 1]$ of Y_m .*
2. *The genus of X_m is $g := q_0(q-1)$.*
3. *The number of \mathbb{F}_q -rational points is $q^2 + 1$, which is maximal as shown by the Serre bound.*
4. *The Suzuki curve X_m is the unique curve (up to \mathbb{F}_q -isomorphism) with properties (2) and (3) above.*
5. *The automorphism group of X_m , as well as of $X_m \times_{\mathbb{F}_q} \bar{\mathbb{F}}_2$, is the Suzuki group $\text{Sz}(q) = {}^2B_2$ of order $q^2(q-1)(q^2+1)$.*
6. *The functions $x, y, z := x^{2q_0+1} - y^{2q_0}$, and $w := xy^{2q_0} - z^{2q_0}$ are regular outside P_∞ with pole orders at P_∞ given by $q, q+q_0, q+2q_0$, and $q+2q_0+1$ respectively.*
7. *The functions t, x, y, z and w give a smooth embedding of X_m into \mathbb{P}^4 .*

The number $N_j(X_m)$ of \mathbb{F}_{q^j} -rational points on the curve can be determined using the zeta function of the curve, or more specifically using the L polynomial, which is the numerator of the zeta function, as follows. By [10, Corollary 5.1.16], if the L -polynomial is $L(X_m, t) = \prod_{k=1}^{2g} (1 - \alpha_k t)$, then

$$N_j(X_m) = q^j + 1 - \sum_{k=1}^{2g} \alpha_k^j. \quad (2.2)$$

For the Suzuki curve, it was shown in [6] that

$$L(X_m, t) = (1 + 2q_0 t + q t^2)^g.$$

The roots of the polynomial $L(X_m, t)$ are $\underbrace{\alpha, \alpha, \dots, \alpha}_{g \text{ times}}$ and $\underbrace{\beta, \beta, \dots, \beta}_{g \text{ times}}$, where

$$\alpha := q_0(-1 + i)$$

and

$$\beta := \bar{\alpha} = q_0(-1 - i).$$

Therefore,

$$N_j(X_m) = q^j + 1 - gq_0(-1 + i) - gq_0(-1 - i) = q^j + 1 + 2gq_0.$$

In the case $j = 1$, we see that $N_1(X_m) = q + 1 - q(q - 1) = q^2 + 1$. We will use these points to construct our codes.

3 The Riemann-Roch space $\mathcal{L}(\ell D)$

In order to construct an AG code whose automorphism group is the full automorphism group $\text{Sz}(q)$ of X_m , we need to choose a divisor that is invariant under the action of $\text{Sz}(q)$ on X_m . Suzuki originally constructed $\text{Sz}(q)$ as a doubly transitive group acting on the curve [11]. So the only way to choose an invariant divisor is to take the set of *all* \mathbb{F}_{q^j} points for some j . The smallest such set of points is the set of \mathbb{F}_q -points.

Consider the divisor $D \in \text{Div}(X_m)$ given by the sum of all \mathbb{F}_q -rational points of X_m . These are the points $P_{\alpha, \beta}$ with affine coordinates (α, β) for any α and β in \mathbb{F}_q , plus the point at infinity. Thus

$$D = P_\infty + \sum_{\alpha, \beta \in \mathbb{F}_q} P_{\alpha, \beta}.$$

Since there are $q^2 + 1$ many \mathbb{F}_q -rational points of X_m , $\deg(D) = q^2 + 1$. Moreover, the divisor D is fixed by $\text{Sz}(q)$, so codes based at D will have $\text{Sz}(q)$ as their automorphism group. In this section, we prove the following theorem, finding an explicit \mathbb{F}_q -basis for the space $\mathcal{L}(\ell D)$, where $\ell \leq q^2 - 1$.

Theorem 3.1. *Let $\ell \in \mathbb{N}$, $\ell \leq q^2 - 1$, and D be defined to be the sum of all \mathbb{F}_q -rational points of X_m . Then,*

$$S := \left\{ \frac{x^a y^b z^c w^d}{(x^q + x)^r} : \begin{array}{l} aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1) \leq rq^2 + \ell, \\ 0 \leq a \leq q - 1, 0 \leq b \leq 1, 0 \leq c \leq q_0 - 1, \\ 0 \leq d \leq q_0 - 1, 0 \leq r \leq \ell \end{array} \right\} \quad (3.1)$$

is a basis for $\mathcal{L}(\ell D)$.

Note that the function $x^q + x$ vanishes at every affine point of X_m and has a pole of order q^2 at P_∞ . Therefore

$$\text{div}(x^q + x) = -q^2 P_\infty + \sum_{\alpha, \beta \in \mathbb{F}_q} P_{\alpha, \beta}.$$

Hence, $\ell D = \ell(q^2 + 1)P_\infty + \text{div}((x^q + x)^\ell)$, i.e., $\ell D \sim \ell(q^2 + 1)P_\infty$. Thus, we have that $\mathcal{L}(\ell D) \simeq \mathcal{L}(\ell(q^2 + 1)P_\infty)$ where the \mathbb{F}_q -isomorphism is given by $f \mapsto f(x^q + x)^\ell$ for $f \in \mathcal{L}(\ell D)$. Thus Theorem 3.1 is equivalent (via $r_{\text{new}} = \ell - r_{\text{old}}$) to the following.

Theorem 3.2. *Let $\ell \in \mathbb{N}$, $\ell \leq q^2 - 1$. Then*

$$S' := \left\{ x^a y^b z^c w^d (x^q + x)^r : \begin{array}{l} aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1) + rq^2 \leq \ell(q^2 + 1) \\ 0 \leq a \leq q - 1, 0 \leq b \leq 1, 0 \leq c \leq q_0 - 1, \\ 0 \leq d \leq q_0 - 1, 0 \leq r \leq \ell \end{array} \right\} \quad (3.2)$$

is a basis for $\mathcal{L}(\ell(q^2 + 1)P_\infty)$.

In order to prove this theorem, we recall a result in [7]. Let $\mathcal{P} \subseteq \mathbb{Z}_{\geq 0}$ be the semigroup generated by the pole orders of the functions x , y , z , and w defined in Proposition 2.1. That is,

$$\mathcal{P} := \langle q, q + q_0, q + 2q_0, q + 2q_0 + 1 \rangle \subseteq \mathbb{Z}_{\geq 0}. \quad (3.3)$$

Proposition 1.6 in [7] is equivalent to the following:

Proposition 3.3. ([7]) *For every integer j ,*

$$\dim_{\mathbb{F}_q}(\mathcal{L}(jP_\infty)) = \#\{n \in \mathcal{P} | n \leq j\}.$$

We are now ready for the proof.

Proof. (Theorem 3.2) Let $f = x^a y^b z^c w^d (x^q + x)^r$ be an element of S' , and let v_∞ be the discrete valuation corresponding to the point P_∞ . Then

$$v_\infty(f) = -[aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1) + rq^2],$$

and f has no other poles. Thus the first inequality in the definition of S' shows that $S' \subseteq \mathcal{L}(\ell(q^2 + 1)P_\infty)$. Thus, in light of Proposition 3.3, it suffices to show that for every $n \in \mathcal{P}$ such that $n \leq \ell(q^2 + 1)$, S' contains exactly one function with a pole of order n at P_∞ . First we show that the valuations at P_∞ of the functions in S' are distinct. Suppose that F_1 and F_2 in S' had the same valuation at infinity, where $F_1 = x^{a_1} y^{b_1} z^{c_1} w^{d_1} (x^q + x)^{r_1}$ and $F_2 = x^{a_2} y^{b_2} z^{c_2} w^{d_2} (x^q + x)^{r_2}$. Then

$$\begin{aligned} a_1 q + b_1(q + q_0) + c_1(q + 2q_0) + d_1(q + 2q_0 + 1) + r_1 q^2 = \\ a_2 q + b_2(q + q_0) + c_2(q + 2q_0) + d_2(q + 2q_0 + 1) + r_2 q^2. \end{aligned} \quad (3.4)$$

We consider (3.4) modulo q_0 . Then,

$$d_1 \equiv d_2 \pmod{q_0}.$$

Since $1 \leq d_1, d_2 \leq q_0 - 1$, it must be that $d_1 = d_2$.

Next, we consider (3.4) modulo $2q_0$. Then,

$$b_1 q_0 + d_1 \equiv b_2 q_0 + d_1 \pmod{2q_0}.$$

Note that $0 \leq b_1, b_2 \leq 1$. Thus, it must be that $b_1 = b_2$.

Next, consider (3.4) modulo q . Since $d_1 = d_2$ and $b_1 = b_2$, we get

$$2c_1 q_0 \equiv 2c_2 q_0 \pmod{q}$$

and therefore $c_1 \equiv c_2 \pmod{q_0}$. Since $0 \leq c_1, c_2 \leq q_0 - 1$, it must be the case that $c_1 = c_2$.

Finally, consider (3.4) modulo q^2 . Then, since $b_1 = b_2$, $c_1 = c_2$, $d_1 = d_2$, we have

$$a_1q \equiv a_2q \pmod{q^2}.$$

Note that $0 \leq a_1, a_2 \leq q - 1$. Thus, it must be that $a_1 = a_2$. This also shows that $r_1 = r_2$. We conclude that if $v_\infty(F_1) = v_\infty(F_2)$, then $F_1 = F_2$.

Now we must show that if $n \leq \ell(q^2 + 1)$ is an element of \mathcal{P} , then there is a function in S' with pole order n at P_∞ . Let n be such an element. By definition,

$$n = aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1) \quad (3.5)$$

for some positive integers a, b, c, d . We need to show that there are a', b', c', d' , and r such that

$$n = a'q + b'(q + q_0) + c'(q + 2q_0) + d'(q + 2q_0 + 1) + rq^2 \quad (3.6)$$

and $0 \leq a' \leq q - 1$, $0 \leq b' \leq 1$, $0 \leq c' \leq q_0 - 1$, $0 \leq d' \leq q_0 - 1$, and $0 \leq r \leq \ell$.

Let d' be the remainder when n is divided by q_0 . Then d' will be in the correct range. Let

$$n_d = \frac{n - d'(q + 2q_0 + 1)}{q_0}.$$

Let b' be the remainder when n_d is divided by 2. Again, b' will be in the correct range. Let

$$n_b = \frac{n_d - b'(2q_0 + 1)}{2}.$$

Let c' be the remainder when n_b is divided by q_0 . Now $0 \leq c' \leq q_0 - 1$. Let

$$n_c = \frac{n_b - c'(q_0 + 1)}{q_0}.$$

Finally, let a' be the remainder when n_c is divided by q , so that $0 \leq a' \leq q - 1$, and let

$$r = \frac{n_c - a'}{q}.$$

Then we can put these back together as follows:

$$\begin{aligned} n &= n_dq_0 + d'(q + 2q_0 + 1) \\ &= (2n_b + b'(2q_0 + 1))q_0 + d'(q + 2q_0 + 1) \\ &= 2q_0n_b + b'(q + q_0) + d'(q + 2q_0 + q) \\ &= 2q_0(q_0n_c + c'(q_0 + 1)) + b'(q + q_0) + d'(q + 2q_0 + q) \\ &= n_cq + c'(q + 2q_0) + b'(q + q_0) + d'(q + 2q_0 + q) \\ &= rq^2 + a'q + c'(q + 2q_0) + b'(q + q_0) + d'(q + 2q_0 + q). \end{aligned}$$

What remains is to show that r is in the correct range. Since $n \leq \ell(q^2 + 1)$, this means that

$$\begin{aligned} n_d &\leq \ell(2qq_0 + \frac{1}{q_0}) \\ n_b &\leq \ell(qq_0 + \frac{1}{2q_0}) \\ n_c &\leq \ell(q + \frac{1}{q}) \\ r &\leq \ell + \frac{\ell}{q^2}. \end{aligned}$$

Since r is an integer and $\ell < q^2$, this means that $r \leq \ell$. Finally, to see that $0 \leq r$ we need first to show that n_d, n_b, n_c are positive integers. Since $n \equiv d' \pmod{q_0}$, we have that $d \equiv d' \pmod{q_0}$ and so we can write $d - d' = t_d q_0$, for some positive integer t_d (note the previous assumption asserts that $d \geq d'$, otherwise we have d already in the required range and we don't need to find n_d). Now we have that

$$\begin{aligned} n_d &:= \frac{n - d'(q + 2q_0 + 1)}{q_0} = \frac{aq + b(q + q_0) + c(q + 2q_0) + (d - d')(q + 2q_0 + 1)}{q_0} \\ &= a(2q_0) + b(2q_0 + 1) + c(2q_0 + 2) + t_d(q + 2q_0 + 1) \end{aligned}$$

which is a positive integer.

Next we have that $n_d \equiv b' \pmod{2}$, so we have $b + t_d \equiv b' \pmod{2}$ and so again we can write it as $b + t_b - b' = 2t_b$, for some positive integer t_b (with the same assumption as before that b is not in the required range $\{0, 1\}$, so $b \geq b'$). Now we have that

$$\begin{aligned} n_b &:= \frac{n_d - b'(2q_0 + 1)}{2} = \frac{a(2q_0 + c(2q_0 + 2) + (b + t_d - b')(2q_0 + 1) + t_d(q))}{2} \\ &= a(q_0) + c(q_0 + 1) + t_b(2q_0 + 1) + t_d q_0^2 \end{aligned}$$

Which is again a positive integer.

Next, we have that $n_b \equiv c' \pmod{q_0}$, so we have $c + t_b \equiv c' \pmod{q_0}$ and we write $c + t_b - c' = t_c q_0$, for some positive integer t_c and we have that

$$\begin{aligned} n_c &:= \frac{n_b - c'(q_0 + 1)}{q_0} = \frac{a(q_0) + (c + t_b - c')(q_0 + 1) + t_b q_0 + t_d q_0^2}{q_0} \\ &= a + t_c(q_0 + 1) + t_b + t_d q_0 \end{aligned}$$

which is a positive integer. Finally, we have $n_c \equiv a' \pmod{q}$ and so we have $n_c - a'$ is multiple of q and thus r is a positive integer. □

Remark 1. The dimension of $\mathcal{L}(\ell D)$ is given by

$$\dim_{\mathbb{F}_q} \mathcal{L}(\ell D) = \ell(q^2 + 1) - q_0(q - 1) + 1, \quad (3.7)$$

which we can see in two ways. First, since $q^2 + 1 > 2q_0(q - 1)$, we have $\deg D > 2g$ and the result follows from the Riemann-Roch theorem. Second, in [7, Appendix A], it is shown

that $\#(\mathbb{N} \setminus \mathcal{P}) = q_0(q-1)$, and an analysis of their proof shows that the largest number in $\mathbb{N} \setminus \mathcal{P}$ is $2q_0(q-1) - 1$. Thus $\#S$ is the number of possibilities for a, b, c, d , and r , minus $\#(\mathbb{N} \setminus \mathcal{P})$.

Theorem 3.1 gives us an explicit basis for $\mathcal{L}(\ell D)$, which we use to construct Suzuki-invariant codes in the next section.

4 Construction and properties of the code $C(E, \ell D)$

As above, let $D \in \text{Div}(X_m)$ be the sum of all \mathbb{F}_q -rational points in X_m . By Theorem 3.1, for $\ell \leq q^2 - 1$ the Riemann-Roch space $\mathcal{L}(\ell D)$ has the \mathbb{F}_q -basis (3.1), and by Remark 1 $\dim_{\mathbb{F}_q} \mathcal{L}(\ell D) = \ell(q^2 + 1) - g + 1 = \ell(q^2 + 1) - q_0(q-1) + 1$.

Now to construct a Suzuki-invariant geometry code, we must choose another set of points, disjoint from D , which is also invariant under $\text{Sz}(q)$. Since we have used all of the \mathbb{F}_q points for D , we must look to points over extensions of \mathbb{F}_q . Consider the field extension \mathbb{F}_{q^4} of \mathbb{F}_q . Let the divisor $E \in \text{Div}(X_m)$ be the sum of all \mathbb{F}_{q^4} -points minus the sum of all \mathbb{F}_q -points. Then, we have

$$n := \deg(E) = N_4(X_m) - N_1(X_m),$$

where $N_4(X_m)$ is given by the formula (2.2), i.e.,

$$N_4(X_m) = q^4 + 1 - g(\alpha^4 + \beta^4) = q^4 + 1 + 2gq^2 = q^4 + 1 + 2q_0q^2(q-1).$$

Therefore, $n = \deg(E) = q^4 + 1 + 2q_0q^2(q-1) - (q^2 + 1) = q^4 + 2q_0q^2(q-1) - q^2$.

Since $\text{Supp}(E) \cap \text{Supp}(D) = \emptyset$ and Theorem 3.1 provides an explicit basis for $\mathcal{L}(\ell D)$, we construct an algebraic geometry code using the divisors E, D as follows. Let P_1, \dots, P_n be all the points in support of E . Define

$$C_{m,\ell} := C_{\mathcal{L}}(E, \ell \cdot D) = \{(f(P_1), f(P_2), \dots, f(P_n)) \in \mathbb{F}_{q^4}^n \mid f \in \mathcal{L}(\ell \cdot D)\}.$$

Then, we have the following theorem.

Theorem 4.1. *Consider the algebraic geometry code*

$$C_{m,\ell} := C_{\mathcal{L}}(E, \ell \cdot D)$$

over \mathbb{F}_{q^4} , where $\ell \leq q^2 - 1$. Then, $C_{m,\ell}$ is an $[n, k, d]$ -linear code, where

$$\begin{aligned} n &= \deg(E) = q^4 + 2q_0q^2(q-1) - q^2, \\ k &:= \dim_{\mathbb{F}_q} \mathcal{L}(\ell \cdot D) = \ell(q^2 + 1) - q_0(q-1) + 1, \\ d &\geq d^* := n - \deg(\ell \cdot D) = n - \ell(q^2 + 1). \end{aligned}$$

Moreover, this code can correct at least $t = \lfloor (d^ - 1)/2 \rfloor$ errors, and has $\text{Sz}(q)$ as its automorphism group.*

Remark 2. Let $S = \{f_1, \dots, f_k\}$ be the \mathbb{F}_q -basis for $\mathcal{L}(\ell D)$ as in Theorem 3.1. Then, the code $C_{m,\ell}$ has generator matrix $G_{m,\ell} := (f_j(P_i))_{1 \leq j \leq k, 1 \leq i \leq n}$.

Proof. The parameters n and k were computed above; d , d^* and t come from the general theory of AG codes. Because we chose D to be an invariant divisor, the code will have the full group $\text{Sz}(q)$ as its automorphism group. \square

Remark 3. It is easy to check, using equation (2.2), that the number of points of X_m over \mathbb{F}_{q^2} and \mathbb{F}_{q^3} are

$$N_2(X_m) = q^2 + 1; \quad N_3(X_m) = q^3 + 1 - q^2(q - 1) = q^2 + 1.$$

Thus if we let E_j be the sum of all \mathbb{F}_{q^j} -points minus the sum of all \mathbb{F}_q -points, then $\deg(E_2) = \deg(E_3) = 0$. Therefore E_4 , which is the E we used above, is the first non-trivial case.

In fact, the Suzuki curve is a maximal curve over \mathbb{F}_{q^4} , meeting the Hasse-Weil bound.

We now focus on the family of codes where $\ell = q^2 - 1$. Denote this family by C_m , i.e., $C_m := C_{m, q^2-1} = C_{\mathcal{L}}(E, (q^2 - 1)D)$. By Theorem 4.1, C_m is a $[n, k, d \geq d^*]$ -linear code, where

$$\begin{aligned} n &= q^4 + 2q_0q^2(q - 1) - q^2, \\ k &= (q^2 - 1)(q^2 + 1) - q_0(q - 1) + 1 = q^4 - q_0(q - 1), \\ d^* &= n - q^4 + 1 = 2q_0q^2(q - 1) - q^2 + 1. \end{aligned}$$

Using the above, C_m has information rate

$$R_m := \frac{k_m}{n_m} = \frac{q^4 - q_0q + q_0}{q^4 + 2q_0q^2(q - 1) - q^2} = \frac{16q_0^8 - 2q_0^3 + q_0}{16q_0^8 + 16q_0^7 - 4q_0^5 - 4q_0^4}.$$

Thus, as $m \rightarrow \infty$, we have $R_m \rightarrow 1$. This shows that these codes are significant because they have very good parameter, explicitly constructed in polynomial-time, with rate asymptotically approaches one, and in many cases cannot be achieved by Reed-Solomon codes.

Example 4.2. The rate gets close to one very quickly. In order to show this, let us consider the following examples:

1. Let $m = 1$; thus, $q = 8, q_0 = 2$. Then, the resulting code $C_1 = C_{1,63}$ is a $[5824, 4082, \geq 1729]$ -linear code over \mathbb{F}_{4096} and can correct up to 864 errors with information rate $R_1 = 0.7008$.
2. Let $m = 2$; thus, $q = 2^5 = 32, q_0 = 4$. Then, the resulting code $C_2 = C_{2,1023}$ is a $[1051679, 1048452, \geq 3104]$ -linear code over $\mathbb{F}_{1048576}$ and can correct at least 1551 errors with information rate $R_2 = 0.996$.

5 Dual code

As before, let D be the sum of all \mathbb{F}_q -points and the divisor E is the sum of all \mathbb{F}_{q^4} -rational points minus all the \mathbb{F}_q -rational points. Next, we study the dual code of the code $C_{m,\ell} := C_{\mathcal{L}}(E, \ell D)$, where $\ell \leq q^2 - 1$.

Recall from [10, Proposition 2.2.10] that the dual of an algebraic geometry code is given by $C_{\mathcal{L}}(E, \ell D)^\perp = C_{\mathcal{L}}(E, E - \ell D + (\eta))$, where η is a Weil differential such that $\nu_{P_i}(\eta) = -1$ and $\text{res}_{P_i}(\eta) = 1$, for all $i = 1, 2, \dots, n$.

In order to find η we first identify the points of $\mathbb{P}_{\mathbb{F}_{q^4}}^1$ whose fiber in X_m via the map induced by x has an \mathbb{F}_{q^4} -rational point. By Proposition 2.1, P_∞ is the unique point above infinity.

We therefore focus on the points that lie in the affine patch of X_m isomorphic to the open affine $t \neq 0$ of the model Y_m . Note that $y^q + y - \alpha^{q^0}(\alpha^q + \alpha)$ factors completely into linear terms over \mathbb{F}_{q^4} for exactly $q^3 + 2gq$ many α 's in \mathbb{F}_{q^4} , and that for the rest of the α 's the polynomial factors into $q/2$ many irreducible components, each of degree 2. By Kummer's criterion [10, Theorem 3.3.7] applied to the equation $y^q + y - x^{q^0}(x^q + x) = 0$, this implies that there are exactly $q^3 + 2gq$ many \mathbb{F}_{q^4} -rational points of $\mathbb{A}_{\mathbb{F}_{q^4}}^1$ that completely split in X_m , whereas the rest of \mathbb{F}_{q^4} -rational points of $\mathbb{A}_{\mathbb{F}_{q^4}}^1$ don't have an \mathbb{F}_{q^4} -rational point in their fiber.

Let T be the set of α 's in \mathbb{F}_{q^4} such that $x = \alpha$ splits, and let $t := \prod_{\alpha \in T} (x - \alpha)$ be viewed as an element of the function field $\kappa(X_m)$ of X_m , and let $\eta := dt/t$.

By the above discussion, every \mathbb{F}_{q^4} -rational point P of X_m except for P_∞ lies above some affine point $Q_\alpha := (x - \alpha)$ of $\mathbb{P}_{\mathbb{F}_{q^4}}^1$ where $\alpha \in T$. Therefore:

$$v_P(t) = e(P|Q_\alpha)v_{Q_\alpha}(t) = 1 \cdot v_{Q_\alpha}\left(\prod_{\alpha \in T} (x - \alpha)\right) = 1.$$

And so:

$$v_P(\eta) = v_P(dt/t) = -1$$

and

$$\text{res}_P(\eta) = \text{res}_P(1/t) = 1$$

Therefore η satisfies the conditions of Proposition 2.2.10 in [10]. We will now compute (η) . Note that t has zeros at all the \mathbb{F}_{q^4} -rational places except at P_∞ , that is,

$$(t)_0 = E + D - P_\infty.$$

Let Q_∞ denote the point at infinity of $\mathbb{P}_{\mathbb{F}_{q^4}}^1$. Then:

$$\begin{aligned} v_{P_\infty}(t) &= v_{P_\infty}\left(\prod_{\alpha \in T} (x - \alpha)\right) = e(P_\infty|Q_\infty)v_{Q_\infty}\left(\prod_{\alpha \in T} (x - \alpha)\right) = -q|T| = -q(q^3 + 2gq) \\ &= -q^4 - 2gq^2. \end{aligned}$$

Therefore $(t)_\infty = (q^4 + 2gq^2)P_\infty$. Therefore,

$$(t) = (t)_0 - (t)_\infty = E + D - P_\infty - (q^4 + 2gq^2)P_\infty.$$

It follows that $(\eta) = (dt/t) = (2g-2)P_\infty - E - D + P_\infty + (q^4 + 2gq^2)P_\infty$. Thus, by [10, Proposition 2.2.10], the dual of $C_{m,\ell} = C_{\mathcal{L}}(E, \ell D)$ is given by $C_{\mathcal{L}}(E, G^\perp)$, where

$$\begin{aligned} G^\perp &= E - \ell D + (\eta) \\ &= E - \ell D + (2g-2)P_\infty - E - D + P_\infty + (q^4 + 2gq^2)P_\infty \\ &= (-1 - \ell)D + (2g-2+1+q^4+2gq^2)P_\infty \\ &= (-1 - \ell)D + (q^2 - 1 + 2g)(q^2 + 1)P_\infty. \end{aligned}$$

Since $D \sim (q^2 + 1)P_\infty$,

$$\begin{aligned} G^\perp &\sim (-1 - \ell)D + (q^2 + 2g - 1)D \\ &\sim (q^2 + 2g - 1 - 1 - \ell)D. \end{aligned}$$

Thus, the dual code of $C_{\mathcal{L}}(E, \ell D)$ is equivalent to the code $C_{\mathcal{L}}(E, (q^2 + 2g - 2 - \ell)D)$.

Moreover, the dual code $C_{\mathcal{L}}(E, (q^2 + 2g - 2 - \ell)D)$ is also of the form $C_{m,\ell'} = C_{\mathcal{L}}(E, \ell' D)$ if $q^2 + 2g - 2 - \ell \leq q^2 - 1$, i.e., whenever $2g - 1 \leq \ell \leq q^2 - 1$. (In which case $\ell' = q^2 + 2g - 2 - \ell$.)

Thus, we obtain the following result.

Proposition 5.1. *If $\ell \leq q^2 - 1$, then the dual code of $C_{\mathcal{L}}(E, \ell D)$ is equivalent to the code $C_{\mathcal{L}}(E, (-1 - \ell + q^2 + 2g - 1)D)$. Moreover, if $2g - 1 \leq \ell$, $C_{m,\ell}^\perp$ is of the form $C_{m,\ell'}$ for $\ell' = q^2 + 2g - 2 - \ell$.*

Remark 4. The code $C_{\mathcal{L}}(E, \ell D)$ is isodual if and only if for the Weil differential above, we have

$$\begin{aligned} 2\ell D - E &= (\eta) \\ 2\ell D - E &= (2g-2)P_\infty - E - D + P_\infty + (q^4 + 2gq^2)P_\infty \\ 2\ell D &= (q^4 + 2gq^2 + 2g - 1)P_\infty - D \\ 2\ell D &\sim (q^2 + 2g - 1)D - D \\ 2\ell &= q^2 + 2g - 2 \\ \ell &= \frac{q^2}{2} + g - 1. \end{aligned}$$

Hence, we have:

1. $C_{\mathcal{L}}(E, \ell D)$ is isodual if and only if $\ell = q^2/2 + g - 1$.
2. $C_{\mathcal{L}}(E, \ell D)$ is iso-orthogonal if and only if $\ell \leq q^2/2 + g - 1$.

Example 5.2. The smallest case of an isodual code in our family is the case $m = 1$ and $\ell = q^2/2 + g - 1 = 8^2/2 + 14 - 1 = 45$. In that case the code $C_{1,45}$ is isodual.

Remark 5. Note that since the codes $C_{\mathcal{L}}(E, \ell D)$ and $C_{\mathcal{L}}(E, \ell(q^2 + 1)P_\infty)$ are equivalent (since $D \sim (q^2 + 1)P_\infty$), the code $C_{m,\ell}$ is a one-point algebraic geometry code.

References

- [1] Chen, C., Duursma, I.: *Geometry Reed-Solomon codes of length 64 and 65 over \mathbb{F}_8* . IEEE Transactions in Information Theory **49** no. 5, 1351-1353 (2003)
- [2] Deligne P., Lusztig G.: *Representations of reductive groups over finite fields*. Ann. of Math. 103, 103–161 (1976)
- [3] Duursma, I., Park S.: *Delta sets for divisors supported in two points*. Finite Fields Appl. **18** no. 5, 865–885 (2012)
- [4] Fuhrmann R., Fernando T.: *On Weierstrass points and optimal curves*. Rend. Circ. Mat. Palermo (2) Suppl. no. 51, 25–46 (1998)
- [5] Giulietti M., Korchmáros G., Torres F.: *Quotient curves of the Suzuki curve*. Acta Arith. **122**. no. 3, 245–274 (2006)
- [6] Hansen J. P.: *Deligne-Lusztig varieties and group codes*. Coding theory and algebraic geometry (Luminy, 1991), 63–81. Lecture Notes in Math. **1518**. Springer, Berlin (1992)
- [7] Hansen J. P., Stichtenoth H.: *Group codes on certain algebraic curves with many rational points*. Appl. Algebra Engrg. Comm. Comput. **1**. no. 1, 67–77 (1990)
- [8] Henn, H.: *Funktionenkörper mit grosser Automorphismengruppe*. J. Reine Angew. Math. **302**, 96–115 (1978)
- [9] Matthews, G.L.: *Codes from the Suzuki function field*. IEEE Trans. Inform. Theory **50**. no. 12, 3298–3302 (2004)
- [10] Stichtenoth, H.: *Algebraic function field and code*. Springer, Berlin (2009)
- [11] Suzuki, M.: *On a class of doubly transitive groups*. Ann. of Math. **75**, 105–145 (1962)

Current authors information:

Abdulla Eid: Department of Mathematics at BTC, University of Bahrain, Bahrain
email: aeid@uob.edu.bh

Hilaf Hasson: Department of Mathematics, Stanford University, Palo Alto, CA 94305, USA
email: hilaf@stanford.edu

Amy Ksir: Department of Mathematics, United States Naval Academy, Annapolis, MD 21402, USA
email: ksir@usna.edu

Justin Peachey: Independent Researcher
email: jdpeachey@gmail.com